Christian Schindelhauer

Freiburg, den 26. Juni 2013
Besprechung 03. Juli 2013

Übungen zur Vorlesung

Systeme II / Rechnernetze

Sommer 2013

Blatt 9

AUFGABE 1: 6 Punkte

Sie möchten das Admin-Passwort eines Online-Forums rekonstruieren und besitzen nur noch den MD5-Hash-Code des Passworts: `e770dac72193f75f8d5a7858bd6a1393`

1. Beschreiben Sie MD5 und diskutieren Sie dessen Sicherheit.
2. Finden Sie das verschlüsselte Passwort, indem Sie ein Programm schreiben, das eine Brute-Force-Attacke durchführt. Sie können hierbei annehmen, dass das Passwort aus 6 Buchstaben besteht und nur die Buchstaben aus {a, b, c, d, e, f, g, h, i, j, 1, 2, 3, 4, 5, 6, 7, 8, 9, #, $} verwendet.
3. Wie kann man die Sicherheit der mit MD5 verschleierten Passwörter erhöhen?

AUFGABE 2: 4 Punkte

Verbinden Sie sich per SSH (PuTTY in Windows) mit den Uniserver. Sie benötigen dazu die Logindaten für ihren Pool-Account. Beobachten Sie dabei den Verbindungsaufbau mit Wireshark und erläutern sie den Nachrichtenaustausch.